On Secret Sharing Schemes, Matroids and Polymatroids[*]

Jaume Martí-Farré, Carles Padró
Dep. de Matemàtica Aplicada 4, Universitat Politècnica de Catalunya, Barcelona, Spain
{jaumem,cpadro}@ma4.upc.edu

October 23, 2007

Abstract

One of the main open problems in secret sharing is the characterization of the access structures of ideal secret sharing schemes. As a consequence of the results by Brickell and Davenport, every one of those access structures is related in a certain way to a unique matroid.

Matroid ports are combinatorial objects that are almost equivalent to matroid-related access structures. They were introduced by Lehman in 1964 and a forbidden minor characterization was given by Seymour in 1976. These and other subsequent works on that topic have not been noticed until now by the researchers interested on secret sharing.

By combining those results with some techniques in secret sharing, we obtain new characterizations of matroid-related access structures. As a consequence, we generalize the result by Brickell and Davenport by proving that, if the information rate of a secret sharing scheme is greater than 2/3, then its access structure is matroid-related. This generalizes several results that were obtained for particular families of access structures.

In addition, we study the use of polymatroids for obtaining upper bounds on the optimal information rate of access structures. We prove that every bound that is obtained by this technique for an access structure applies to its dual structure as well.

Finally, we present lower bounds on the optimal information rate of the access structures that are related to two matroids that are not associated with any ideal secret sharing scheme: the Vamos matroid and the non-Desargues matroid.

Key words. Secret sharing, Information rate, Ideal secret sharing schemes, Ideal access structures, Matroids, Polymatroids.

1 Introduction

1.1 The Problems

A *secret sharing scheme* is a method to distribute a *secret value* into *shares* in such a way that only some *qualified subsets* of *participants* are able to recover the secret from their shares. Secret sharing schemes were independently introduced by Shamir [34] and Blakley [5]. Only *unconditionally secure perfect secret sharing schemes* will be considered in this paper. That is, the shares of the participants in a non-qualified subset must not contain any information about the secret value.

[*] This work was partially supported by the Spanish Ministry of Education and Science under projects TIC2003-00866 and TSI2006-02731. This work was done while the second author was in a sabbatical stay at CWI, Amsterdam. This stay was funded by the *Secretaría de Estado de Educación y Universidades* of the Spanish Ministry of Education. A preliminary version of this work appeared in *Fourth IACR Theory of Cryptography Conference TCC 2007, Lecture Notes in Computer Science* **4392** (2007) 273–290.

The family of the qualified subsets is the *access structure* of the scheme, which is supposed to be *monotone increasing*, that is, every subset containing a qualified subset must be qualified. Then an access structure is determined by its *minimal qualified subsets*.

The complexity of a secret sharing scheme can be measured by the length of the shares. In all secret sharing schemes, the length of every share is greater than or equal to the length of the secret [20]. A secret sharing scheme is said to be *ideal* if all shares have the same length as the secret.

The qualified subsets of a *threshold access structure* are those having at least a fixed number of participants. Shamir's construction [34] provides an ideal scheme for every threshold access structure. Even though there exists a secret sharing scheme for every access structure [18], in general some shares must be much larger than the secret [12, 13].

This paper deals with the optimization of the complexity of secret sharing schemes for general access structures.

The characterization of the *ideal access structures*, that is, the access structures of ideal secret sharing schemes, is one of the main open problems in that direction. Brickell and Davenport [10] discovered important connections of this problem with matroid theory. The main definitions and basic facts about secret sharing schemes, matroids, and polymatroids are presented in Section 2. Table 1, at the end of the paper, may be helpful to the readers that are not familiar with the concepts that are discussed here.

A necessary condition for an access structure to be ideal is obtained from the results by Brickell and Davenport [10]. They proved that every ideal secret sharing scheme on a set P of participants univocally determines a matroid $\mathcal{M}$ on the set $Q = P \cup \{D\}$, where $D \notin P$ is a special participant, usually called *dealer*. In addition, the access structure Γ of the ideal scheme is determined by this matroid. Specifically, the minimal qualified subsets of Γ are

$$\min \Gamma = \{A \subseteq P \,:\, A \cup \{D\} \text{ is a circuit of } \mathcal{M}\}.$$

Therefore, every ideal access structure is *matroid-related*, that is, it can be defined in this way from a matroid. This necessary condition is not sufficient, because there exist matroids that cannot be defined from any ideal secret sharing scheme [27, 33], and hence the access structures that are related to these matroids are not ideal.

The matroids that are obtained from ideal secret sharing schemes are generally called *secret sharing matroids*, but we prefer to call them *ideal secret sharing representable matroids*, or *iss-representable matroids* for short. This is due to the fact that an ideal secret sharing scheme can be seen as a representation of its associated matroid.

Brickell [9] proposed a special class of ideal schemes, the *vector space secret sharing schemes*. The matroids that are associated with these ideal schemes are precisely the linearly representable ones. Therefore, all linearly representable matroids are iss-representable. This implies that the representation by ideal secret sharing schemes is a generalization of the linear representation of matroids. In addition, every access structure that is related to a linearly representable matroid is ideal. These access structures are called *vector space access structures*. This sufficient condition is not necessary, because there exist iss-representable matroids that are not linearly representable [35].

As a consequence of the results by Brickell and Davenport [10] the open problem of characterizing the access structures of ideal secret sharing schemes can be splitted into the following two open problems.

Open Problem 1.1. Characterize the matroid-related access structures.

Open Problem 1.2. Characterize the ideal secret sharing representable matroids.

Surprisingly enough, almost all authors interested on secret sharing, including the ones of this paper, have been unaware that matroid-related access structures were studied before secret sharing was invented. Of course, a different name was used: *matroid ports*.

A *clutter* on a set P is a family Λ of subsets of P such that there do not exist two different subsets $A, B \in \Lambda$ with $A \subset B$. A clutter Λ on P is a *matroid port* if there exists a matroid $\mathcal{M}$ on $Q = P \cup \{D\}$, where $D \notin P$, such that

$$\Lambda = \{A \subseteq P \,:\, A \cup \{D\} \text{ is a circuit of } \mathcal{M}\}.$$

Therefore, an access structure is matroid-related if an only if the clutter formed by its minimal qualified subsets is a matroid port. Matroid ports were introduced by Lehman [21] in 1964 to solve the Shannon switching game. Seymour [32] presented in 1976 a characterization of matroid ports by excluded minors that is based on a previous characterization of matroid ports due to Lehman [22]. As a consequence, an answer to Problem 1.1 is obtained.

A more general open problem in secret sharing is to determine the complexity of the best secret sharing scheme for any given access structure. For instance, we can try to maximize the *information rate*, which is the ratio between the length in bits of the secret and the maximum length of the shares. The *optimal information rate* of an access structure Γ, which is denoted by $\rho(\Gamma)$, is defined as the supremum of the information rates of all secret sharing schemes with access structure Γ. Clearly, $0 < \rho(\Gamma) \leq 1$, and $\rho(\Gamma) = 1$ if Γ is ideal.

Open Problem 1.3. Determine the value of $\rho(\Gamma)$ or, at least, improve the known bounds on this function.

Duality has been defined for matroids, for linear codes, and for access structures. It plays an important role in the considered problems. For instance, if an access structure is related to a matroid, its dual is related to the dual matroid. One can consider the dual of a linear secret sharing scheme by identifying it with a linear code. A linear scheme with the same information rate for the dual access structure is obtained in this way. Nevertheless, it is not known whether the dual of an ideal access structure is ideal as well. In addition, the relation between the optimal information rates of an access structure and its dual is equally an open problem.

1.2 Our Results

Because of their important implications to the problems we are considering here, one of the main goals of this paper is to point out the results by Lehman [21, 22] and Seymour [32] on matroid ports to researchers interested on secret sharing. We think that they will be very useful to obtain new general results on the problems we are considering here as well as to solve them for particular families of access structures.

One of our main results, Theorem 4.5, is a new characterization of matroid-related access structures in terms of the existence of *independent sequences*. These sequences are combinatorial configurations that were introduced in [6,30] to obtain upper bounds on the optimal information rate. Our characterization is obtained by combining Seymour's characterization of matroid ports [32] with the fact that the Shannon entropy defines a polymatroid over a set of random variables [15, 16]. As a corollary of Theorem 17 we obtain a generalization of the result by Brickell and Davenport [10]. Namely, they proved that the access structure of every ideal secret sharing scheme is matroid-related, and we prove that this is so for every secret sharing scheme with information rate greater than 2/3. This is the main result in this paper.

Theorem 1.4. *The access structure of every secret sharing scheme with information rate greater than* $2/3$ *is matroid-related.*

Our proof for this theorem, as well as the ones for the results we apply in it, do not rely on the result by Brickell and Davenport [10]. Moreover, except for the relation between entropy and polymatroids, those proofs use only combinatorial techniques. Therefore, we can say that we present here a new, almost purely combinatorial proof for that important result.

Theorem 1.4 explains a gap property that has been observed in some particular classes of access structures that have been previously studied, in which every access structure is either ideal or has optimal information at most 2/3. So, there is no access structure Γ with $2/3 < \rho(\Gamma) < 1$ in these families. Specifically, this has been proved for the access structures on sets of four [36] and five [19] participants, the ones defined by graphs [7,10,12], the bipartite ones [30], the ones with three or four minimal qualified subsets [24], the ones with intersection number equal to one [26], and for a special class of homogeneous structures with rank three [23]. This fact was proved by methods that seemed to be specific to every one of those families, and hence it was not clear to which extent this result could be generalized. Since in all those families every matroid-related access structure is ideal, this gap property is a direct consequence of Theorem 1.4, which implies that $\rho(\Gamma) \leq 2/3$ if Γ is not matroid-related. Therefore, we generalize and explain a phenomenon that had been observed in several particular situations. Moreover, our result can be applied to other families that have been studied previously as, for instance, the weighted threshold access structures [3] and the access structures with rank three [25].

In addition, we present in Section 3 a new result about the use of polymatroids to obtain upper bounds on the information rate, a technique that was introduced by Csirmaz [13]. Specifically, we prove that every bound on the optimal information rate of a given access structure that can be obtained by using polymatroids applies also to the dual access structure. In order to do that, we define in a suitable way the *dual* of a polymatroid. The interest of this result is that, for the first time, we present a connection between the complexities of the secret sharing schemes for an access structure and the ones for its dual that is not restricted to linear schemes.

Finally, Section 5 is devoted to present lower bounds on the optimal information rate of the access structures related to the Vamos matroid and the non-Desargues matroid. Since these matroids are not iss-representable, the related access structures are not ideal. We prove that the optimal information rate of the access structures related to the Vamos matroid is at least 2/3, while this parameter is at least 3/4 for the structures related to the non-Desargues matroid. The only previously known results on the optimal information rate of non-ideal matroid-related access structures have been presented in a recent work by Beimel and Livne [2]. They give lower bounds on the length of the shares in secret sharing schemes for the access structures related to the Vamos matroid.

1.3 Related Work

As a sequel of the results by Brickell and Davenport [10], there is a number of works dealing with Problem 1.2. The Vamos matroid was the first matroid that was proved to be non-iss-representable. This was done by Seymour [33] and different proofs were given later by Simonis and Ashikhmin [35] and Beimel and Livne [2]. An infinite family of non-iss-representable matroids was given by Matúš [27]. As we said before, all linearly representable matroids are iss-representable [9]. The first example of an iss-representable matroid that is not linearly representable, the non-Pappus matroid, was presented in [35].

A number of important results and interesting ideas for future research on Problem 1.2 can be found in the works by Simonis and Ashikhmin [35] and Matúš [27]. The first one deals with the geometric structure that lies behind iss-representations of matroids. The second one analyzes the algebraic properties that the matroid induces in all its iss-representations. These properties make it possible to find some restrictions on the iss-representations of a given matroid and, in some cases, to exclude the existence of such representations. By using these tools, Matúš [27] presented an infinite family of non-iss-representable matroids with rank three.

One of the most important results on the optimization of the complexity of secret sharing schemes for general access structures is the fact that nonlinear secret sharing schemes are in general more efficient than the linear ones. By using the results and techniques in [1, 17], Beimel and Weinreb [4] presented families of access structures for which there exist nonlinear secret sharing schemes whose complexity is polynomial on the number of participants while the complexity of the best linear schemes is not polynomial.

Lower bounds on the optimal information rate of wide families of access structures can be found by applying the different techniques to construct secret sharing schemes with high information rate given in [8, 11, 31, 37, 38]. Upper bounds on this parameter have been found by using Information Theory [6, 7, 12]. In particular, Capocelli, De Santis, Gargano, and Vaccaro [12] presented for the first time bounds smaller than 1 on the optimal information rate. Specifically, they showed access structures whose optimal information rates are at most 2/3. Csirmaz [13] proved that every secret sharing scheme defines a polymatroid that is related to the access structure and he observed that those upper bounds on the optimal information rate could be derived from this fact. A general combinatorial method to find upper bounds, the *independent sequence method*, was given in [6] and was improved in [30]. However, there exists a wide gap between the best known upper and lower bounds on the optimal information rate for most access structures.

2 Basics on Secret Sharing, Matroids, and Polymatroids

The reader is referred to [36] for an introduction to secret sharing and to [29, 39] for general references on matroid theory. The book by Welsh [39] contains a chapter about polymatroids. Table 1 summarizes the connections between some of the concepts that are introduced here.

Let Q be a finite set of *participants* and $D \in Q$ a special participant called *dealer*. Consider a finite set E with a probability distribution on it. For every $i \in Q$, consider a finite set E_i and a surjective mapping $\pi_i \colon E \to E_i$. Those mappings induce random variables on the sets E_i. Let $H(E_i)$ denote the Shannon entropy of one of these random variables. For a subset $A = \{i_1, \ldots, i_r\} \subseteq Q$, we write $H(A)$ for the joint entropy $H(E_{i_1} \ldots E_{i_r})$, and a similar convention is used for conditional entropies as, for instance, in $H(E_j|A) = H(E_j|E_{i_1} \ldots E_{i_r})$.

The mappings π_i define a *secret sharing scheme* Σ with *access structure* Γ on the set $P = Q - \{D\}$ of participants if $H(E_D) > 0$ and $H(E_D|A) = 0$ if $A \in \Gamma$ while $H(E_D|A) = H(E_D)$ if $A \notin \Gamma$. In this situation, every random choice of an element $\mathbf{x} \in E$, according to the given probability distribution, results in a *distribution of shares* $((s_i)_{i \in P}, s)$, where $s_i = \pi_i(\mathbf{x}) \in E_i$ is the *share* of the participant $i \in P$ and $s = \pi_D(\mathbf{x}) \in E_D$ is the *shared secret value.*

A participant is said to be *redundant* in an access structure if there is no minimal qualified set containing it. An access structure is *connected* if there is not any redundant participant in it.

The ratio $\rho(\Sigma) = H(E_D)/\max_{i \in P} H(E_i)$ is called the *information rate* of the scheme Σ, and the *optimal information rate* $\rho(\Gamma)$ of the access structure Γ is the supremum of the information rates of all secret sharing schemes with access structure Γ. It is not difficult to check that $H(E_i) \geq H(E_D)$ for every non-redundant participant $i \in P$, and hence $\rho(\Sigma) \leq 1$. Secret sharing schemes with $\rho(\Sigma) = 1$ are said to be *ideal* and their access structures are called *ideal* as well. Of course, $\rho(\Gamma) = 1$ for every ideal access structure Γ.

If the sets E and E_i are vector spaces over some finite field $\mathbb{K}$, the mappings π_i are linear mappings, and the uniform probability distribution is considered in E, we say that Σ is a $\mathbb{K}$-

linear secret sharing scheme. The linear schemes in which $E_i = \mathbb{K}$ for every $i \in Q$ are ideal and they are called $\mathbb{K}$*-vector space secret sharing schemes*. Their access structures are called $\mathbb{K}$*-vector space access structures*. Observe that there exist ideal linear schemes that are not vector space secret sharing schemes. In such schemes, $\dim E_i = \dim E_D > 1$ for every $i \in P$.

We notate $\mathcal{P}(Q)$ for the power set of Q. Given a secret sharing scheme Σ on the set $P = Q - \{D\}$, consider the mapping $h \colon \mathcal{P}(Q) \to \mathbb{R}$ defined by $h(X) = H(X)/H(E_D)$. This mapping satisfies the following properties [13].

1. $h(\emptyset) = 0$, and

2. h is *monotone increasing*: if $X \subseteq Y \subseteq Q$, then $h(X) \leq h(Y)$, and

3. h is *submodular*: if $X, Y \subseteq Q$, then $h(X \cup Y) + h(X \cap Y) \leq h(X) + h(Y)$, and

4. for every $X \subseteq Q$, either $h(X \cup \{D\}) = h(X) + 1$ or $h(X \cup \{D\}) = h(X)$.

A *polymatroid* is any pair $\mathcal{S} = (Q, h)$ satisfying the first three properties. Polymatroids satisfying the fourth property as well will be called here *D-secret sharing polymatroids*, or *D-ss-polymatroids* for short. Therefore, every secret sharing scheme Σ defines a D-ss-polymatroid $\mathcal{S} = \mathcal{S}(\Sigma) = (Q, h)$. Nevertheless, there exist D-ss-polymatroids that are not associated with any secret sharing scheme.

For a D-ss-polymatroid $\mathcal{S} = (Q, h)$, we consider the access structure

$$\Gamma_D(\mathcal{S}) = \{A \subseteq P \,:\, h(A \cup \{D\}) = h(A)\}.$$

Clearly, the access structure of a secret sharing scheme Σ is the one defined in this way by the associated polymatroid $\mathcal{S}(\Sigma)$. Since there exists a secret sharing scheme for every access structure Γ, all access structures are of the form $\Gamma_D(\mathcal{S})$ for some D-ss-polymatroid $\mathcal{S}$. Nevertheless, different D-ss-polymatroids can define the same access structure.

A *matroid* can be defined as a polymatroid $\mathcal{M} = (Q, h)$ with the following additional property.

4′. $h(X) \in \mathbb{Z}$ and $0 \leq h(X) \leq |X|$ for every $X \subseteq Q$, or, equivalently, for every $X \subseteq Q$ and $x \in Q$, either $h(X \cup \{x\}) = h(X) + 1$ or $h(X \cup \{x\}) = h(X)$.

We need to recall now some terminology and basic facts about matroids. For a matroid $\mathcal{M} = (Q, r)$ (we change from h to r because this is the usual notation for matroids), the set Q and the mapping r are called, respectively, the *ground set* and the *rank function* of the matroid $\mathcal{M}$. The value $r(X)$ is called the *rank* of the subset X while the *rank of the matroid* $\mathcal{M}$ is defined to be $r(\mathcal{M}) = r(Q)$. A subset $X \subseteq Q$ is said to be *independent* if $r(X) = |X|$. The *dependent* subsets are those that are not independent. A *circuit* is a minimally dependent subset while a *basis* is a maximally independent subset. All bases have the same number of elements, which coincide with the rank of the matroid.

As a consequence of the results by Brickell and Davenport [10], if Σ is an ideal scheme, then the polymatroid $\mathcal{S} = \mathcal{S}(\Sigma)$ is a matroid and, hence, $\mathcal{S}$ is a j-ss-polymatroid for every $j \in Q$. Moreover, by considering $(\pi_i(\mathbf{x}))_{i \in Q - \{j\}}$ as shares of the secret value $\pi_j(\mathbf{x})$, the scheme Σ defines an ideal secret sharing scheme with access structure $\Gamma_j(\mathcal{S})$ on the set of participants $Q - \{j\}$. We say that Γ is a *matroid-related* access structure if $\Gamma = \Gamma_D(\mathcal{M})$ for some matroid $\mathcal{M}$. It is not difficult to check that this definition is equivalent to the one we gave in the Introduction. Observe that the results by Brickell and Davenport [10] imply that all ideal access structures are matroid-related.

Let $\mathbb{K}$ be a finite field and let M be a $r_0 \times n$ matrix with entries in $\mathbb{K}$. If $|Q| = n$ and the points in Q are put in a one-to-one correspondence with the columns of M, a matroid $\mathcal{M}$ on the set Q is obtained by considering that the rank of a subset $X \subseteq Q$ is equal to the rank of the corresponding columns of M. In this situation, we say that the matrix M is a $\mathbb{K}$-*representation* of the matroid $\mathcal{M}$. The matroids that can be defined in this way are called *linearly representable*. Observe that linearly representable matroids coincide with the ones that are obtained from vector space secret sharing schemes and their related access structures are precisely the vector space access structures. The matroids that are associated with an ideal linear secret sharing scheme are called *multilinearly representable*, a class that contains the linearly representable matroids. The non-Pappus matroid is not linearly representable [29], but it was proved to be multilinearly representable in [35]. The existence of iss-representable matroids that are not multilinearly representable is an open problem.

The matroid $\mathcal{M}$ is said to be *connected* if, for every two different points $i, j \in Q$, there exists a circuit C with $i, j \in C$. As a consequence of [29, Proposition 4.1.2], the matroid $\mathcal{M}$ is connected if and only if the access structure $\Gamma_D(\mathcal{M})$ is connected. A connected matroid is determined by the circuits that contain some given point [21]. Therefore, if Γ is a matroid-related connected access structure, there exists a unique matroid $\mathcal{M}$ with $\Gamma = \Gamma_D(\mathcal{M})$.

3 Polymatroids and Optimal Information Rate

Most of the upper bounds on the optimal information rate that have been given until now were obtained by information-theoretical arguments. Specifically, by using basic properties of the Shannon entropy function. Csirmaz [13] pointed out that all those results are based solely on the so-called *Shannon inequalities* on the entropy of subsets of variables and, hence, they can be deduced from the fact that every secret sharing scheme defines a D-ss-polymatroid related to the access structure.

If $\mathcal{S} = (Q, h)$ is a polymatroid, we define $\sigma(\mathcal{S}) = \max\{h(\{x\}) : x \in Q\}$. For every access structure Γ, we consider the value $\kappa(\Gamma) = \inf \sigma(\mathcal{S})$, where the infimum is taken over all D-ss-polymatroids $\mathcal{S}$ with $\Gamma = \Gamma_D(\mathcal{S})$. The upper bounds on the optimal information rate that can be obtained by using polymatroids (that is, by using Shannon inequalities) are based on the following proposition.

Proposition 3.1. *The optimal information rate of every access structure* Γ *is upper bounded by* $\rho(\Gamma) \leq 1/\kappa(\Gamma)$.

Proof. Let Σ be a secret sharing scheme with access structure Γ and let $\mathcal{S}$ be the D-ss-polymatroid defined by Σ. Then $\rho(\Sigma) = 1/\sigma(\mathcal{S}) \leq 1/\kappa(\Gamma)$. □

Therefore, upper bounds on $\rho(\Gamma)$ can be found by deriving lower bounds on $\kappa(\Gamma)$ from combinatorial properties of the access structure. Actually, $1/\kappa(\Gamma)$ is the best upper bound that can be obtained by this technique. Since $\kappa(\Gamma)$ deals only with the properties of the D-ss-polymatroids $\mathcal{S}$ such that $\Gamma = \Gamma_D(\mathcal{S})$, and some of these polymatroids may not be associated with any secret sharing scheme, there can exist access structures Γ such that $\rho(\Gamma) < 1/\kappa(\Gamma)$. As far as we know, no examples of access structures in this situation are known, but Theorem 3.4 gives some intuition supporting their existence.

Since $\kappa(\Gamma) = 1$ if Γ is matroid-related, it is clear that no upper bounds on the optimal information rate of matroid-related access structures can be found by using this method.

As far as we know, the only known upper bounds that do not fit this pattern are the one given by Gál [17], which was improved in [28], and the one presented by Beimel and Livne [2]. The first one applies only to linear secret sharing schemes and it is the basis for proving the separation between the complexities of linear and nonlinear schemes [1, 4]. The second one applies to the access structures related to the Vamos matroid.

As an example of the kind of results that are obtained by using polymatroids, we present the *independent sequence method*, which was introduced in [6] and was improved in [30]. Let Γ be an access structure on a set of participants P. Consider $A \subseteq P$ and an increasing sequence of subsets $B_1 \subseteq \cdots \subseteq B_m \subseteq P$. We say that $(B_1, \ldots, B_m \,|\, A)$ is an *independent sequence* in Γ with *length* m and *size* s if $|A| = s$ and, for every $i = 1, \ldots, m$, there exists $X_i \subseteq A$ such that $B_i \cup X_i \in \Gamma$, while $B_m \notin \Gamma$ and $B_{i-1} \cup X_i \notin \Gamma$ if $i \geq 2$. The independent sequence method is based on the following result. We notice that this theorem was not stated in [6, 30] in terms of polymatroids, but in terms of the entropy function. The proof in [6] is easily adapted to this new statement.

Theorem 3.2. ([6, 30]) *Let Γ be an access structure on the set P. Let $\mathcal{S} = (Q, h)$ be a D-ss-polymatroid such that $\Gamma = \Gamma_D(\mathcal{S})$. If there exists in Γ an independent sequence $(B_1, \ldots, B_m \,|\, A)$ with length m and size s, then $h(A) \geq m$. As a consequence, $\kappa(\Gamma) \geq m/s$ and $\rho(\Gamma) \leq s/m$.*

The following corollary of that theorem points out that independent sequences can be used in the characterization of matroid-related access structures. Actually, the converse of this result will be proved in Section 4.

Corollary 3.3. *An access structure is not matroid-related if it admits an independent sequence with length m and size $s < m$.*

The next result by Csirmaz [13] points out the limitations of the use of polymatroids to find upper bounds on the optimal information rate.

Theorem 3.4. ([13]) *If Γ is an access structure on a set P of participants with $|P| = n$, then $\kappa(\Gamma) \leq n$.*

Proof. It is not difficult to prove that there exists a D-ss-polymatroid $\mathcal{S} = (Q, h)$ with $\Gamma = \Gamma_D(\mathcal{S})$ such that $h(X) = n + (n-1) + \cdots + (n-(k-1))$ for every subset of participants $X \subseteq P$ with $|X| = k$. □

By taking into account the known methods to construct secret sharing schemes, it is against intuition to suppose that there can exist, for every access structure, a secret sharing scheme such that the length of the shares is around n times the length of the secret. Therefore, as a consequence of Theorem 3.4, it seems that the optimal information rate of an access structure will be in general much smaller than $1/\kappa(\Gamma)$, the best upper bound that can be obtained by using polymatroids. Nevertheless, besides the Shannon inequalities, the properties of the entropy function imply other inequalities, the so-called *non-Shannon inequalities*. Thus, it might be possible to find better upper bounds on the optimal information rate than the ones derived from Proposition 3.1 by using information theory. This may be the case for matroid-related access structures as well.

Anyway, the polymatroid technique has proved to be very useful when studying some particular families of access structures. In some cases the obtained upper bounds are tight or, at least, close to the best known lower bounds. In the following we prove a positive result for the polymatroid technique. Namely, we prove in Theorem 3.8 that the bounds that are obtained by this technique for an access structure apply also to its dual.

Before presenting our result, we recall some facts about dual access structures and dual matroids. The *dual* of the access structure Γ on the set P is defined as the access structure $\Gamma^* = \{A \subseteq P \,:\, P - A \notin \Gamma\}$. If $\mathcal{M} = (Q, r)$ is a matroid, the mapping $r^* \colon \mathcal{P}(Q) \to \mathbb{Z}$ defined by

$r^*(X) = |X| - r(Q) + r(Q - X)$ is the rank function of a matroid $\mathcal{M}^* = (Q, r^*)$, which is called the *dual* of the matroid $\mathcal{M}$. Since $\Gamma_D(\mathcal{M}^*) = (\Gamma_D(\mathcal{M}))^*$, the dual of a matroid-related access structure is matroid-related. If Σ is an ideal secret sharing scheme with access structure Γ, then there exists a linear scheme Σ^* with access structure Γ^* and information rate $\rho(\Sigma^*) = \rho(\Sigma)$ [14]. Actually, Σ can be seen as a linear code, and the linear scheme Σ^* is the one constructed from the dual code. As a consequence, if a matroid is linearly or multilinearly representable, the same applies to the dual matroid. Nevertheless, it is not known whether the dual of an iss-representable matroid is iss-representable, and the relation between $\rho(\Gamma)$ and $\rho(\Gamma^*)$ is an open problem too. Our result, Theorem 3.8, deals with this open problem. Specifically, we prove that the upper bounds for $\rho(\Gamma)$ that are obtained by the polymatroid technique apply also to $\rho(\Gamma^*)$.

There exist several inequivalent ways to define the dual of a polymatroid [39] and we have to choose the suitable one to prove our result. Specifically, if $\mathcal{S} = (Q, h)$ is a polymatroid, we consider the *dual polymatroid* $\mathcal{S}^* = (Q, h^*)$, where $h^* \colon \mathcal{P}(Q) \to \mathbb{R}$ is defined by $h^*(X) = \sum_{x \in X} h(\{x\}) - h(Q) + h(Q - X)$. This definition generalizes the duality that is usually considered for matroids. Clearly, if $\mathcal{M} = (Q, r)$ is a *loopless* matroid, that is, with $r(\{x\}) = 1$ for every $x \in Q$, then the dual matroid of $\mathcal{M}$ coincides with the dual polymatroid. We prove in the next lemma that $\mathcal{S}^*$ is actually a polymatroid, and we describe in Lemma 3.6 the relation between the dual of a D-ss-polymatroid and the dual of the corresponding access structure.

Lemma 3.5. *$\mathcal{S}^* = (Q, h^*)$ is a polymatroid.*

Proof. Obviously, $h^*(\emptyset) = 0$. Take a subset $X \subseteq Q$ and a point $y \notin X$. Since $h(\{y\}) + h(Q - (X \cup \{y\})) \geq h(Q - X)$, we get that $h^*(X \cup \{y\}) \geq h^*(X)$. Therefore, h^* is monotone increasing. Finally, consider two arbitrary subsets $X, Y \subseteq Q$. Then from the definition of h^* and the submodularity of h,

$$h^*(X) + h^*(Y) - h^*(X \cup Y) - h^*(X \cap Y) =$$

$$= h(Q - X) + h(Q - Y) - h(Q - (X \cup Y)) - h(Q - (X \cap Y)) \geq 0.$$

This proves that h^* is submodular. □

Lemma 3.6. *Let $\mathcal{S} = (Q, h)$ be a D-ss-polymatroid. Assume that $\Gamma_D(\mathcal{S}) \neq \emptyset$ and $\emptyset \notin \Gamma_D(\mathcal{S})$. Then $\mathcal{S}^* = (Q, h^*)$ is also a D-ss-polymatroid and $\Gamma_D(\mathcal{S}^*) = (\Gamma_D(\mathcal{S}))^*$.*

Proof. Let $\Gamma = \Gamma_D(\mathcal{S})$. Since $\emptyset \notin \Gamma$ and $P = Q - \{D\} \in \Gamma$, we have that $h(\{D\}) = 1$ and $h(P) = h(Q)$, and hence $h^*(\{D\}) = 1$. Consider a subset $X \subseteq P$. Then $h^*(X \cup \{D\}) = h(\{D\}) + \sum_{x \in X} h(\{x\}) - h(Q) + h(P - X)$. If $X \in \Gamma^*$, then $P - X \notin \Gamma$ and $h(P - X) = h(Q - X) - 1$. In this case, $h^*(X \cup \{D\}) = h^*(X)$. Analogously, if $X \notin \Gamma^*$ then $h(P - X) = h(Q - X)$, and hence $h^*(X \cup \{D\}) = h^*(X) + 1$. □

To be precise, the polymatroid $\mathcal{S}^*$ is properly a dual of $\mathcal{S}$, in the sense that $\mathcal{S}^{**} = \mathcal{S}$, if and only if $h(Q - \{x\}) = h(Q)$ for every $x \in Q$. The polymatroids satisfying this property will be said to be *normalized*. In addition, we need some technical results that are given in the next lemma, whose proof is an easy exercise.

Lemma 3.7. *Let $\mathcal{S} = (Q, h)$ be a polymatroid. Then the following properties hold.*

1. *The polymatroid $\mathcal{S}^* = (Q, h^*)$ is normalized.*

2. *$h^{**}(X) \leq h(X)$ for every $X \subseteq Q$.*

3. $\mathcal{S}$ is normalized if and only if $\mathcal{S}^{**} = \mathcal{S}$.

4. If $\mathcal{S}$ is normalized, then $h^*(\{x\}) = h(\{x\})$ for every $x \in Q$.

Theorem 3.8. *Let Γ be an access structure with $\Gamma \neq \emptyset$ and $\emptyset \notin \Gamma$, and let Γ^* be its dual. Then $\kappa(\Gamma) = \kappa(\Gamma^*)$.*

Proof. Let Γ be an access structure. Consider the sets of real numbers $\Omega(\Gamma) = \{\sigma(\mathcal{S}) : \Gamma = \Gamma_D(\mathcal{S})\}$ and $\widehat{\Omega}(\Gamma) = \{\sigma(\mathcal{S}) : \mathcal{S}$ is normalized, $\Gamma = \Gamma_D(\mathcal{S})\}$. If $\mathcal{S}$ is a D-ss-polymatroid such that $\Gamma = \Gamma_D(\mathcal{S})$, then $\mathcal{S}^{**}$ is normalized, $\Gamma = \Gamma_D(\mathcal{S}^{**})$ and $\sigma(\mathcal{S}^{**}) \leq \sigma(\mathcal{S})$. Therefore, $\kappa(\Gamma) = \inf \Omega(\Gamma) = \inf \widehat{\Omega}(\Gamma)$. The proof is concluded by taking into account that $\widehat{\Omega}(\Gamma) = \widehat{\Omega}(\Gamma^*)$. □

4 On the Characterization of Matroid-Related Access Structures

4.1 A Theorem by Seymour

Let Γ be an access structure on a set P and take a subset $Z \subseteq P$. We define the access structures $\Gamma \setminus Z$ and Γ/Z on the set $P - Z$ by $\Gamma \setminus Z = \{A \subseteq P - Z : A \in \Gamma\}$ and $\Gamma/Z = \{A \subseteq P - Z : A \cup Z \in \Gamma\}$. Every access structure that can be obtained from Γ by repeatedly applying the operations $\setminus$ and $/$ is called a *minor of the access structure* Γ. If Z_1 and Z_2 are disjoint subsets then $(\Gamma \setminus Z_1)/Z_2 = (\Gamma/Z_2) \setminus Z_1$, and $(\Gamma \setminus Z_1) \setminus Z_2 = \Gamma \setminus (Z_1 \cup Z_2)$, and $(\Gamma/Z_1)/Z_2 = \Gamma/(Z_1 \cup Z_2)$. Therefore, every minor of Γ is of the form $(\Gamma \setminus Z_1)/Z_2$ for some disjoint subsets $Z_1, Z_2 \subseteq P$. In addition, $(\Gamma \setminus Z)^* = \Gamma^*/Z$ and $(\Gamma/Z)^* = \Gamma^* \setminus Z$.

We can consider as well *minors* of matroids and polymatroids. Let $\mathcal{S} = (Q, h)$ be a polymatroid. Given a subset $Z \subseteq Q$, we define the polymatroids $\mathcal{S} \setminus Z = (Q - Z, h_{\setminus Z})$ and $\mathcal{S}/Z = (Q - Z, h_{/Z})$, where $h_{\setminus Z}(X) = h(X)$ and $h_{/Z}(X) = h(X \cup Z) - h(Z)$ for every $X \subseteq Q - Z$. It is not difficult to prove that, if $\mathcal{S}$ is a D-ss-polymatroid and $\Gamma = \Gamma_D(\mathcal{S})$, then for every $Z \subseteq P$, both $\mathcal{S} \setminus Z$ and $\mathcal{S}/Z$ are D-ss-polymatroids and $\Gamma \setminus Z = \Gamma_D(\mathcal{S} \setminus Z)$ and $\Gamma/Z = \Gamma_D(\mathcal{S}/Z)$. Moreover, if $\mathcal{M} = (Q, r)$ is a matroid, then $\mathcal{M} \setminus Z$ and $\mathcal{M}/Z$ are matroids as well. The following proposition is a direct consequence of all these considerations.

Proposition 4.1. *Every minor of a matroid-related access structure is matroid-related.*

We introduce now the forbidden minors in the characterization by Seymour. The set of participants of the access structures Φ and $\widehat{\Phi}$ is $P = \{p_1, p_2, p_3, p_4\}$. The minimal qualified subsets of Φ are $\{p_1, p_2\}$, $\{p_2, p_3\}$ and $\{p_3, p_4\}$, while the minimal qualified subsets $\widehat{\Phi}$ are $\{p_1, p_2\}$, $\{p_2, p_3\}$, $\{p_2, p_4\}$ and $\{p_3, p_4\}$. For every $s \geq 3$, the set of participants of the access structure Ψ_s is $P = \{p_1, \ldots, p_s, p_{s+1}\}$ and its minimal qualified subsets are $\{p_1, \ldots, p_s\}$ and $\{p_i, p_{s+1}\}$ for every $i = 1, \ldots, s$. Observe that $\Phi^* \cong \Phi$ and $\Psi_s^* = \Psi_s$. The minimal qualified subsets of $\widehat{\Phi}^*$ are $\{p_1, p_3, p_4\}$, $\{p_2, p_3\}$ and $\{p_2, p_4\}$.

The forbidden minor characterization of matroid ports by Seymour is stated here in our terminology.

Theorem 4.2. (Seymour [32]) *An access structure is matroid-related if and only if it has no minor isomorphic to Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_s with $s \geq 3$.*

4.2 Generalizing the Result by Brickell and Davenport

New characterizations of matroid-related access structures are given in Theorem 4.5. They are obtained by combining Theorem 4.2 with the results in Section 3. As a consequence we obtain Theorem 1.4, a generalization of the result by Brickell and Davenport [10].

We need to introduce two technical results that are used in the proof of Theorem 4.5. First, the independent sequence method we have described in Section 3 has a good behavior with respect to minors, and second, all the forbidden minors in Seymour's characterization admit an independent sequence with length $m = 3$ and size $s = 2$.

Lemma 4.3. *Let Γ' be a minor of an access structure Γ. If there exists in Γ' an independent sequences with length m and size s, then the same occurs for Γ.*

Proof. Consider disjoint subsets $Z_1, Z_2 \subseteq P$ such that $\Gamma' = (\Gamma \setminus Z_1)/Z_2$. Suppose that $(B_1, \dots, B_m \,|\, A)$ is an independent sequence with length m and size $s = |A|$ in Γ'. Then $(B_1 \cup Z_2, \dots, B_m \cup Z_2 \,|\, A)$ is an independent sequence in Γ. □

Proposition 4.4. *Every one of the access structures Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$, and Ψ_s with $s \geq 3$ admits an independent sequence with length $m = 3$ and size $s = 2$.*

Proof. We are going to consider sequences $(B_1, B_2, B_3 \,|\, a_1 a_2)$ with $B_1 \subseteq B_2 \subseteq B_3 \subseteq P$ and $a_1, a_2 \in P$. Such a sequence will be independent in the access structure Γ if the subsets $B_1 \cup \{a_1, a_2\}$, $B_2 \cup \{a_1\}$ and $B_3 \cup \{a_2\}$ are in Γ while $B_1 \cup \{a_1\}$, $B_2 \cup \{a_2\}$ and B_3 are not in Γ. The sequence $(\emptyset, \{p_1\}, \{p_1, p_4\} \,|\, p_2 p_3)$ is independent for both Φ and $\widehat{\Phi}$, while an independent sequence for $\widehat{\Phi}^*$ is $(\emptyset, \{p_4\}, \{p_1, p_4\} \,|\, p_2 p_3)$. Finally, $(\emptyset, \{p_s\}, \{p_2, \dots, p_s\} \,|\, p_{s+1} p_1)$ is an independent sequence in Ψ_s. □

Theorem 4.5. *Let Γ be an access structure. Then the following statements are equivalent.*

1. *Γ is matroid-related.*
2. *There does not exist in Γ any independent sequence with length m and size $s < m$.*
3. *There does not exist in Γ any independent sequence with length $m = 3$ and size $s = 2$.*
4. *$\kappa(\Gamma) < 3/2$.*

Proof. If Γ is matroid-related, then $\kappa(\Gamma) = 1$ and, by Corollary 3.3, there does not exist in Γ any independent sequence with length m and size $s < m$. In addition, by Theorem 3.2, there does not exist in Γ any independent sequence with length $m = 3$ and size $s = 2$ if $\kappa(\Gamma) < 3/2$. Finally, if Γ is not matroid-related, then there exists a minor Γ' of Γ that is isomorphic to one of the forbidden minors in Theorem 4.2. From Proposition 4.4, Γ' admits an independent sequence with length $m = 3$ and size $s = 2$ and, by Lemma 4.3, the same occurs with Γ. □

Two direct consequences of Theorem 4.5 are stated in Corollary 4.6. Our main result, Theorem 1.4, is proved from the second one. As we said before, we have obtained in this way a generalization of the important result by Brickell and Davenport [10], who proved that the access structure of every ideal secret sharing scheme is matroid-related. Moreover, since the result by Brickell and Davenport has not been used in the proof of Theorem 4.5, we have presented here an alternative proof for it.

Corollary 4.6. *Let Γ be an access structure. Then the following statements hold.*

1. *Γ is matroid-related if and only if $\kappa(\Gamma) = 1$.*
2. *If Γ is not matroid-related, then $\kappa(\Gamma) \geq 3/2$, and hence $\rho(\Gamma) \leq 2/3$.*

This result implies a gap in the values of $\kappa(\Gamma)$. Namely, there does not exist any access structure Γ with $1 < \kappa(\Gamma) < 3/2$. This gap does not mean that the corresponding gap appears in the values of the optimal information rate $\rho(\Gamma)$. Specifically, the existence of non-ideal matroid-related access structures Γ with $2/3 < \rho(\Gamma) < 1$ is an open problem.

5 On Non-Ideal Matroid-Related Access Structures

Since there exist matroids that are not iss-representable, there are matroid-related access structures that are not ideal. Very little is known about the optimal information rate of these structures. We cannot find upper bounds by the techniques in Section 3 because $\kappa(\Gamma) = 1$ if Γ is matroid-related. By using other techniques, upper bounds have been given by Beimel and Livne [2]. We present here some lower bounds on the optimal information rate of the access structures related to the Vamos matroid and the non-Desargues matroid.

Our lower bounds are obtained by using the *λ-decomposition technique* introduced by Stinson [38]. Specifically, we use the following proposition, which is a corollary of [38, Theorem 2.1].

Proposition 5.1. *Let Γ be an access structure on a set P of participants, and let $(\Gamma_1, \dots, \Gamma_m)$ be a collection of substructures of Γ (that is, $\Gamma_i \subseteq \Gamma$) such that $\Gamma = \bigcup_{i=1}^m \Gamma_i$. The substructures Γ_i may not be connected. For every $i = 1, \dots, m$, consider the set $P_i \subseteq P$ of participants that appear in some minimal qualified subset of the substructure Γ_i, and, for every $x \in P$, consider $w(x) = |\{i : x \in P_i\}|$ and take $w = \max_{x \in P} w(x)$. For every minimal qualified subset $A \in \min \Gamma$, consider $\lambda(A) = |\{i : A \in \Gamma_i\}|$ and take $\lambda = \min_{A \in \min \Gamma} \lambda(A)$. Assume that there exists a finite field $\mathbb{K}$ such that all substructures Γ_i are $\mathbb{K}$-vector space access structures. Then, there exists for the access structure Γ a $\mathbb{K}$-linear secret sharing scheme with set of secrets $E_0 = \mathbb{K}^\lambda$ and information rate equal to λ / w.*

The *Vamos matroid* $\mathcal{V}$ is the matroid on the set $Q_1 = \{v_1, \dots, v_8\}$ such that its bases are all sets with cardinality 4 except the following five: $\{v_1, v_2, v_3, v_4\}$, $\{v_1, v_2, v_5, v_6\}$, $\{v_3, v_4, v_5, v_6\}$, $\{v_3, v_4, v_7, v_8\}$ and $\{v_5, v_6, v_7, v_8\}$. The Vamos matroid is not iss-representable [33] and, hence, the access structures related to it are not ideal. In a recent work, Beimel and Livne [2] prove that, for every secret sharing scheme realizing one of these access structures with domain of the secrets of size k, the size of the domain of the shares is at least $k + \Omega(\sqrt{k})$. Observe that this bound does not exclude that the optimal information rate of these structures may be equal to one, because $\rho(\Gamma)$ is the *supremum* of the information rates of the schemes realizing Γ.

The *non-Desargues matroid* $\mathcal{N}$ is the matroid with rank 3 on a set with 10 points determined by a non-Desargues configuration on a projective plane. That is, take three different lines L_1, L_2, L_3 that meet in a point p_0 and, on the line L_i, two different points $q_i, r_i \neq p_0$. Finally, consider the points s_{12}, s_{23}, and s_{31}, where s_{ij} is the intersection of the lines $q_i q_j$ and $r_i r_j$. If such a configuration has been taken on a projective plane over a field, the points s_{12}, s_{23} and s_{31} must be collinear by the Desargues' Theorem. The non-Desargues matroid is defined by this configuration but considering that the three points s_{ij} are not collinear. That is, the ground set of $\mathcal{N}$ is $Q_2 = \{p_0, q_1, q_2, q_3, r_1, r_2, r_3, s_{12}, s_{23}, s_{31}\}$, and the bases are all subsets with three points that are not supposed to be collinear. As a consequence of the Desargues' Theorem, this matroid is not linearly representable. Moreover, Matúš [27] proved that it is not iss-representable.

Theorem 5.2. *If an access structure is related to the Vamos matroid or the non-Desargues matroid, then its optimal information rate is at least* $3/4$.

Proof. Let $\mathcal{B}$ be the family of bases of the Vamos matroid $\mathcal{V}$. On the same ground set $Q_1 = \{v_1, \dots, v_8\}$ as the Vamos matroid, consider, for every $i = 1, \dots, 4$, the matroid $\mathcal{M}_i$ with family of bases $\mathcal{B}_i$, where $\mathcal{B}_1 = \mathcal{B} \cup \{\{v_1, v_2, v_3, v_4\}\}$, $\mathcal{B}_2 = \mathcal{B} \cup \{\{v_3, v_4, v_5, v_6\}\}$, $\mathcal{B}_3 = \mathcal{B} \cup \{\{v_3, v_4, v_7, v_8\}\}$, and $\mathcal{B}_4 = \mathcal{B} - \{\{v_1, v_2, v_7, v_8\}\}$. Consider the access structures $\Gamma = \Gamma_{v_3}(\mathcal{V})$ and $\Gamma_i = \Gamma_{v_3}(\mathcal{M}_1)$, where $i = 1, \dots, 4$. Then

- $\min \Gamma_1 = \min \Gamma - \{\{v_1, v_2, v_4\}\}$,
- $\min \Gamma_2 = \min \Gamma - \{\{v_4, v_5, v_6\}\}$,

Access structures of...		**Access structures related to...**
SSS with $\rho > 2/3$	$\Longrightarrow$ [here] $\Longleftarrow$?	Matroids
		$\Uparrow$ $\not\Downarrow$ [27,33]
Ideal SSS	$\Longleftrightarrow$ [10]	Iss-representable matroids
		$\Uparrow$ $\Downarrow$?
Ideal linear SSS	$\Longleftrightarrow$	Multilinearly representable matroids
		$\Uparrow$ $\not\Downarrow$ [35]
Vector space SSS	$\Longleftrightarrow$ [9]	Linearly representable matroids

Table 1:

- $\min \Gamma_3 = \min \Gamma - \{\{v_4, v_7, v_8\}\}$, and
- $\min \Gamma_4 = \min \Gamma - \{\{v_1, v_2, v_7, v_8\}\}$.

Since the matroids $\mathcal{M}_i$ are linearly representable over finite fields of all characteristics, the access structures Γ_i are $\mathbb{K}$-vector space access structures for some finite field $\mathbb{K}$. By applying Proposition 5.1 to the collection $(\Gamma_1, \dots, \Gamma_4)$, we obtain a $\mathbb{K}$-linear secret sharing scheme for Γ with information rate $\lambda/w = 3/4$. Every access structure $\Gamma_{v_i}(\mathcal{V})$ related to the Vamos matroid is isomorphic to $\Gamma_{v_3}(\mathcal{V})$ or to $\Gamma_{v_1}(\mathcal{V})$. In addition, $\Gamma_{v_1}(\mathcal{V}) \cong (\Gamma_{v_3}(\mathcal{V}))^*$. Therefore, for every $v_i \in Q_1$, there exists a linear secret sharing scheme with access structure $\Gamma_{v_i}(\mathcal{V})$ and information rate equal to 3/4.

Let $D \in Q_2$ be an arbitrary point in the ground set of the non-Desargues matroid $\mathcal{N}$ and consider the access structure $\Gamma = \Gamma_D(\mathcal{N})$ on the set $P_2 = Q_2 - \{D\}$ of participants. There exists a finite field $\mathbb{K}$ such that, for every $x \in P_2$, the matroid $\mathcal{N} \setminus \{x\}$ is $\mathbb{K}$-representable and, hence, $\Gamma \setminus \{x\}$ is a $\mathbb{K}$-vector space access structure. Therefore, we can apply Proposition 5.1 to the collection formed by the nine access structures $\{\Gamma \setminus \{x\}\}_{x \in P_2}$. Clearly $w = 8$ and, since every minimal qualified subset of Γ has at most three participants, $\lambda = 6$. Therefore, a linear secret sharing scheme for Γ with information rate equal to $\lambda/w = 6/8 = 3/4$ is obtained. □

6 Open Problems

The known results about the connection between secret sharing and matroids, including our main result, are summarized in Table 1. Equally, some open problems appear there. The following open problem was posed in [24, 26].

Open Problem 6.1. Is there any access structure Γ with $2/3 < \rho(\Gamma) < 1$?

From Theorem 1.4, if such an access structure exists, it must be matroid-related. We proved before that there exist non-ideal matroid-related access structures Γ with $\rho(\Gamma) \geq 3/4$. Nevertheless, it is possible that $\rho(\Gamma) = 1$ even if Γ is not ideal. Observe that the results in [2] about the length of the shares for the access structures related to the Vamos matroid do not imply an affirmative answer to Problem 6.1. Actually, very little is known about the optimal information rate of non-ideal matroid-related access structures.

Open Problem 6.2. Is there any matroid-related access structure Γ with $\rho(\Gamma) < 1$? And with $\rho(\Gamma) \leq 2/3$?

The existence of ideal access structures that are not realized by any ideal linear secret sharing scheme is another unsolved question, which is equivalent to the following open problem.

Open Problem 6.3. Is there any iss-representable matroid that is not multilinearly representable?

Even though the existence of access structures Γ with $\rho(\Gamma) < 1/\kappa(\Gamma)$ is quite natural from Theorem 3.4, no actual example is known.

Open Problem 6.4. Present an access structure Γ with $\rho(\Gamma) < 1/\kappa(\Gamma)$.

Acknowledgments

The second author thanks Ronald Cramer, Bert Gerards, Robbert de Haan and Lex Schrijver for useful discussions, comments, and suggestions. Thanks to Lex Schrijver, who pointed out the existence of the paper by P.D. Seymour on matroid ports [32], and to Bert Gerards, who independently found the construction in Theorem 3.4.

References

[1] A. Beimel, Y. Ishai. On the power of nonlinear secret sharing schemes. *SIAM J. Discrete Math.* **19** (2005) 258–280.

[2] A. Beimel, N. Livne. On Matroids and Non-ideal Secret Sharing. *Third Theory of Cryptography Conference, TCC 2006. Lecture Notes in Comput. Sci.* **3876** (2006) 482–501.

[3] A. Beimel, T. Tassa, E. Weinreb. Characterizing Ideal Weighted Threshold Secret Sharing. *Second Theory of Cryptography Conference, TCC 2005. Lecture Notes in Comput. Sci.* **3378** (2005) 600–619.

[4] A. Beimel, E. Weinreb. Separating the power of monotone span programs over different fields. *SIAM J. Comput.* **34** (2005) 1196–1215.

[5] G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings*. **48** (1979) 313–317.

[6] C. Blundo, A. De Santis, R. De Simone, U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Des. Codes Cryptogr.* **11** (1997) 107–122.

[7] C. Blundo, A. De Santis, L. Gargano, U. Vaccaro. On the information rate of secret sharing schemes. *Advances in Cryptology - CRYPTO'92. Lecture Notes in Comput. Sci.* **740** (1993) 148–167.

[8] C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro. Graph decompositions and secret sharing schemes. *J. Cryptology* **8** (1995) 39–64.

[9] E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.* **9** (1989) 105–113.

[10] E.F. Brickell, D.M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology* **4** (1991) 123–134.

[11] E.F. Brickell, D.R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. Cryptology* **5** (1992) 153–166.

[12] R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro. On the size of shares of secret sharing schemes. *J. Cryptology* **6** (1993) 157–168.

[13] L. Csirmaz. The size of a share must be large. *J. Cryptology* **10** (1997) 223–231.

[14] S. Fehr. Efficient Construction of the Dual Span Program. Manuscript.

[15] S. Fujishige. Entropy functions and polymatroids—combinatorial structures in information theory. *Electron. Comm. Japan* **61** (1978) 14–18.

[16] S. Fujishige. Polymatroidal Dependence Structure of a Set of Random Variables. *Information and Control* **39** (1978) 55–72.

[17] A. Gál. A characterization of span program size and improved lower bounds for monotone span programs. *Proceedings of 30th ACM Symposium on the Theory of Computing, STOC 1998* (1998) 429–437.

[18] M. Ito, A. Saito, T. Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87* (1987) 99–102.

[19] W.-A. Jackson, K.M. Martin. Perfect secret sharing schemes on five participants. *Des. Codes Cryptogr.* **9** (1996) 267–286.

[20] E.D. Karnin, J.W. Greene, M.E. Hellman. On secret sharing systems. *IEEE Trans. Inform. Theory* **29** (1983) 35–41.

[21] A. Lehman. A solution of the Shannon switching game. *J. Soc. Indust. Appl. Math.* **12** (1964) 687–725.

[22] A. Lehman. Matroids and Ports. *Notices Amer. Math. Soc.* **12** (1965) 356–360.

[23] J.Martí-Farré, C. Padró. Secret sharing schemes on sparse homogeneous access structures with rank three. *Electronic Journal of Combinatorics* **11(1)** (2004) Research Paper 72, 16 pp. (electronic).

[24] J. Martí-Farré, C. Padró. Secret sharing schemes with three or four minimal qualified subsets. *Des. Codes Cryptogr.* **34** (2005) 17–34.

[25] J.Martí-Farré, C. Padró. Ideal secret sharing schemes whose minimal qualified subsets have at most three participants. *Fifth Conference on Security and Cryptography for Networks, SCN 2006. Lecture Notes in Comput. Sci.* **4116** (2006) 201–215.

[26] J. Martí-Farré, C. Padró. Secret sharing schemes on access structures with intersection number equal to one. *Discrete Applied Mathematics* **154** (2006) 552–563.

[27] F. Matúš. Matroid representations by partitions. *Discrete Math.* **203** (1999) 169–194.

[28] V. Nikov, S. Nikova, B. Preneel. On the Size of Monotone Span Programs. *Fourth Conference on Security in Communication Networks - SCN 2004. Lecture Notes in Comput. Sci.* **3352** (2004) 252–265.

[29] J.G. Oxley. *Matroid theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.

[30] C. Padró, G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. Inform. Theory* **46** (2000) 2596–2604.

[31] C. Padró, G. Sáez. Lower bounds on the information rate of secret sharing schemes with homogeneous access structure. *Inform. Process. Lett.* **83** (2002) 345–351.

[32] P.D. Seymour. A forbidden minor characterization of matroid ports. *Quart. J. Math. Oxford Ser.* **27** (1976) 407–413.

[33] P.D. Seymour. On secret-sharing matroids. *J. Combin. Theory Ser. B* **56** (1992) 69–73.

[34] A. Shamir. How to share a secret. *Commun. of the ACM* **22** (1979) 612–613.

[35] J. Simonis, A. Ashikhmin. Almost affine codes. *Des. Codes Cryptogr.* **14** (1998) 179–197.

[36] D.R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.* **2** (1992) 357–390.

[37] D.R. Stinson. New general lower bounds on the information rate of secret sharing schemes. *Advances in Cryptology - CRYPTO'92. Lecture Notes in Comput. Sci.* **740** (1993) 168-182.

[38] D.R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Trans. Inform. Theory* **40** (1994) 118–125.

[39] D.J.A. Welsh. *Matroid Theory*. Academic Press, London, 1976.